ABSTRACT

Security Protocol

A system has a local client application (10) and a communications stack (20, 14) by which the local application can communicate with remote peer applications on other systems. The communications stack includes a transport entity (14) for providing transport services, and a transport-independent, session-level security entity (20) logically positioned above the transport entity and visible to the local application. The security entity has a key-exchange handshake protocol engine (24) for conducting a handshake with a peer security entity (30) associated with a particular remote application (12) with which the local application (10) wishes to communicate, this handshake involving the exchange of key-related data for use in generating session keys. The security entity (20) also has a secure channel engine (25) for enabling messages to be passed between the local application and the target remote application with authentication and/or encryption. During the key-exchange handshake, the handshake protocol engine (24) exchanges attribute justifications, in the form of one or more certificates, with its peer whereby to enable verification by each system that the application (12;10) being contacted has the particular attributes, if any, required by its own application (10;12).

(Fig. 1)